776 F.2d at 1240-41 (dismissing case where "the parties' ability to prove the truth or falsity of the alleged libel" either risked or depended on the disclosure of state secrets). Likewise, if the privilege "'deprives the *defendant* of information that would otherwise give the defendant a valid defense to the claim, then the court may grant summary judgment to the defendant.'" *Kasza*, 133 F.3d at 1166 (quoting *Bareford*, 973 F.2d at 1141) (emphasis in original).

(U) Thus, if state secrets are needed to decide a particular claim, then wholly apart from the "very subject matter" issue, the Court must enter summary judgment against the Plaintiffs since the evidence needed to adjudicate the merits is unavailable. *See Kasza,* 133 F.3d at 1176 (affirming entry of summary judgment for the United States on state secrets privilege grounds); *Zuckerbraun*, 935 F.2d at 547 (where effect of state secrets privilege assertion is to prevent plaintiff from establishing a *prima facie* case, summary judgment under Rule 56 is appropriate on the ground that either the plaintiff, who bears the burden of proof, lacks sufficient evidence to carry that burden, or that the exclusion of evidence precludes the defendant from establishing a valid defense).[9]

(U) As set forth below, facts as to which the DNI has asserted privilege render the very subject matter of this case a state secret. For example, facts concerning whether or not the Plaintiffs were subject to the alleged intelligence activities are essential to deciding this case, and because Plaintiffs cannot make that showing, the case must be dismissed for lack of jurisdiction. *See Halkin I* and *II, supra.* Similarly, facts concerning any alleged intelligence activities are needed to decide the merits of Plaintiffs' claims, including facts demonstrating that the NSA does not undertake the "dragnet" of content surveillance that Plaintiffs allege, under the TSP or otherwise.

---

[9] **(U)** On occasion, courts have merged the "very subject matter" and "evidentiary" impacts of the privilege and have ruled that *because* certain evidence is essential to make a *prima facie* case or a defense, the very subject matter of the case is a state secret. Thus, in *Kasza*, the Ninth Circuit observed that "[n]ot only does the state secrets privilege bar [plaintiff] from establishing her *prima facie* case on any of her eleven claims, but any further proceedings in this matter would jeopardize national security." *See* 133 F.3d at 1170; *see also Farnsworth Cannon, Inc. v. Grimes,* 635 F.2d 268, 281 (4th Cir. 1980) (en banc) ("It is evident that any attempt on the part of the plaintiff to establish a prima facie case would so threaten disclosure of state secrets that the overriding interest of the United States and the preservation of its state secrets precludes any further attempt to pursue this litigation."); *Zuckerbraun*, 935 F.2d at 547-48 (state secrets needed to address all factual questions related to defendants' liability rendered the "very subject matter" a state secret because "there is no evidence available to the appellant to establish a prima facie case."); *Fitzgerald*, 776 F.2d at 1242, 1244 (outlining elements of defamation claim and testimony needed to address them in concluding that the very subject matter was a state secret).

(U) Thus, there are two issues for the Court to decide. First, granting his judgment the "utmost deference," has the Director of National Intelligence demonstrated that there is at least a reasonable danger that disclosure of the privileged information will cause harm to the national security? Second, is the privileged information needed to litigate this case? As set forth below, the answer to both questions is clearly yes, and dismissal is therefore required.

II. (U) THE UNITED STATES HAS PROPERLY ASSERTED THE STATE SECRETS PRIVILEGE IN THIS CASE.

(U) The United States has properly asserted the state secrets privilege in this case. The Director of National Intelligence, J. Michael McConnell, who bears statutory authority as head of the United States Intelligence Community to protect intelligence sources and methods, *see* 50 U.S.C. § 403-1(i)(l),[10] has formally asserted the state secrets privilege after personal consideration of the matter. *See Reynolds,* 345 U.S. at 7-8. DNI McConnell has submitted an unclassified declaration and an *in camera, ex parte* classified declaration, both of which state that the disclosure of the intelligence information, sources, and methods described therein would cause exceptionally grave harm to the national security of the United States. See Public and *In Camera* Declarations of J. Michael McConnell, Director of National Intelligence. Based on this assertion of privilege by the head of the United States Intelligence Community, the Government's claim of privilege has been properly lodged.

---

[10] **(U)** *See* 50 U.S.C. § 401a(4) (including the NSA in the United States "Intelligence Community").

III. (U) INFORMATION SUBJECT TO THE STATE SECRETS PRIVILEGE IS NECESSARY TO ADJUDICATE PLAINTIFFS' CLAIMS AND, THUS, THIS ACTION CANNOT PROCEED.

(U) As noted above, once the state secrets privilege is asserted, the Court must evaluate the consequences of that assertion on the case. Here, state secrets are "so central to the subject matter of the litigation that any attempt to proceed will threaten disclosure of the privileged matters." *Fitzgerald*, 776 F.2d at 1241-42. Indeed, Plaintiffs can prove neither their standing nor their claims, and Defendants cannot present a full defense, without the privileged information. *See Kasza,* 133 F.3d at 1166. Specifically, adjudicating each of Plaintiffs' claims would necessarily require: (1) confirming or denying that the named Plaintiffs have been subject to any alleged activities; and (2) disclosing the nature and scope of alleged intelligence activities, sources, and methods of the NSA, including facts needed to show whether or not the "dragnet" of domestic communications alleged by Plaintiffs actually exists. Because such information cannot be disclosed without causing exceptionally grave damage to the national security, every stage of this case—either for Plaintiffs to prove their claims or for Defendants to defend them—directly implicates privileged information.

A. (U) Whether or Not Plaintiffs Have Standing Cannot be Established or Refuted Without the Disclosure of State Secrets and Harm to National Security.

(U) The fundamental, threshold issue of Plaintiffs' standing cannot be adjudicated without state secrets. As is well known, the Constitution "limits the jurisdiction of federal courts to 'Cases' and 'Controversies,'" and "the core component of standing is an essential and unchanging part of th[is] case-or-controversy requirement." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 559-60 (1992). Plaintiffs, of course, bear the burden of establishing standing and must, at an "irreducible constitutional minimum," demonstrate (1) an injury-in-fact, (2) a causal connection between the injury and the conduct complained of, and (3) a likelihood that the injury will be redressed by a favorable decision. *Id.* In meeting that burden, the named Plaintiffs must demonstrate an actual or imminent—not speculative or hypothetical—injury that is particularized as to them; they cannot rely on alleged injuries to unnamed members of a purported class. *See, e.g., Warth v. Seldin*, 422 U.S. 490, 502 (1975) (the named plaintiffs in an action "must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent"). Moreover, to obtain prospective relief, Plaintiffs must show that they are "immediately in danger of sustaining some direct injury" as the result of the challenged conduct. *City of Los Angeles v. Lyons,* 461 U.S. 95, 102 (1983); *O'Shea v. Littleton,* 414 U.S. 488, 495-96 (1974).[11]

(U) A plaintiff must demonstrate Article III standing for "each claim he seeks to press," *DaimlerChrysler Corp. v. Cuno*, ___ U.S. ___, 126 S. Ct. 1854, 1867 (2006), and must further establish "prudential" standing by showing that "the constitutional or statutory provision on which [each] claim rests properly can be understood as granting persons in the plaintiff's position a right to judicial relief." *Warth*, 422 U.S. at 499-500. To do so, a plaintiff normally "'must assert his own legal rights and interests, and cannot rest his claim to relief on the legal rights or interests of third parties.'" *Smelt v. County of Orange*, 447 F.3d 673, 682 (9th Cir.)

---

[11] **(U)** Standing requirements demand the "strictest adherence" when, like here, constitutional questions are presented and "matters of great national significance are at stake." *Elk Grove Unified Sch. Dist. v. Newdow,* 542 U.S. 1, 11 (2004); *see also Raines v. Byrd,* 521 U.S. 811, 819-20 (1997) ("[O]ur standing inquiry has been especially rigorous when reaching the merits of the dispute would force us to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional."); *Schlesinger v. Reservists Comm. to Stop the War*, 418 U.S. 208, 221 (1974) ("[W]hen a court is asked to undertake constitutional adjudication, the most important and delicate of its responsibilities, the requirement of concrete injury further serves the function of insuring that such adjudication does not take place unnecessarily.").

(quoting *Valley Forge Christian Coll. v. Ams. United for Separation of Church & State*, 454 U.S. 464, 474-75 (1982)), *cert. denied,* ___ U.S. ___, 127 S. Ct. 396 (2006). To advance a statutory claim, a plaintiff must show that his particular injury "fall[s] within 'the zone of interests to be protected or regulated by the statute'" in question. *Smelt*, 447 F.3d at 683 (quoting *Valley Forge Christian Coll.*, 454 U.S. at 474-75)..

(U) Here, the state secrets privilege prevents Plaintiffs from establishing, and Defendants from refuting, any injury because it bars proof of whether Plaintiffs have been subject to the alleged surveillance activities.[12] As discussed, the Government's privilege assertion covers, *inter alia*, (1) any information tending to confirm or deny whether the Plaintiffs were subject to any of the alleged intelligence activities at issue, and (2) any information concerning the alleged activities, including program facts demonstrating that the TSP was limited to one-end foreign al Qaeda-related communications and was not the "dragnet" that Plaintiffs allege. *See* Public McConnell Decl. ¶ 11. Without these facts—the disclosure of which would harm national security for reasons explained by the DNI and NSA Director—Plaintiffs cannot establish any alleged injury that is fairly traceable to the Defendants.

(U) It is important to emphasize the procedural posture of the Government's pending motion as it pertains to Plaintiffs' standing. Whether the Plaintiffs can establish their standing is not merely a question to be decided on the pleadings. Regardless of whether Plaintiffs adequately allege injury to get past the pleading stage, the United States, through this motion, has specifically put at issue whether the named Plaintiffs will be able to sustain their burden of *proving* a concrete, personal injury *as a factual matter* in light of the state secrets privilege assertion.[13] At this stage, Plaintiffs cannot rest on general allegations in their complaints, but must be able to set forth specific facts by affidavit or evidence that would support their standing to obtain the relief sought. *See Lewis v. Casey*, 518 U.S. 343, 358 (1996) (quoting *Lujan*, 504 U.S. at 561). The issue raised by the Government's motion is whether that will be possible where the DNI has properly asserted privilege over facts tending to confirm or deny the application of alleged intelligence activities to particular individuals, including the named Plaintiffs in this case. Because the DNI has set forth reasonable grounds to protect such information, the facts needed to establish or refute the Plaintiffs' standing cannot be disclosed and the case cannot proceed.[14] This is not an issue that can be deferred. If Plaintiffs' claims of injury cannot be proved without disclosing state secrets and harming national security—and we submit they cannot—then judgment must be entered in favor of the Defendants now.

---

[12] **(U)** The focus herein is on Plaintiffs' inability to prove standing because it is their burden to demonstrate jurisdiction. *See Lujan*, 504 U.S. at 561. Dismissal of this action, however, is also required for the equally important reason that Defendants would not be able to present any evidence disproving standing on any claim without revealing information covered by the state secrets privilege assertion (*e.g.*, whether or not a particular person's communications were intercepted). *See Halkin I*, 598 F.2d at 11 (rejecting plaintiffs' argument that the acquisition of a plaintiff's communications may be presumed from the existence of a name on a watchlist, because "such a presumption would be unfair to the individual defendants who would have no way to rebut it").

---

[13] **(U)** The Court can dismiss this case on the pleadings under the "very subject matter" prong of the state secrets privilege. The Government's summary judgment motion is made in the alternative because, if the Court declines to dismiss on that ground, the questions of whether the state secrets privilege precludes Plaintiffs from proving their standing or making a *prima facie* case, or Defendants from presenting a defense, can also be considered as summary judgment questions. *See Zuckerbraun*, 935 F.2d at 547. Indeed, the Government's summary judgment motion places the burden on Plaintiffs to prove their standing and to make out a *prima facie* case without state secrets, which they cannot do.

[14] **(U)** In *Hepting*, the United States argued, as it has here, that the plaintiffs would be unable to establish standing absent state secrets. In addressing that issue, the Court referred to its prior conclusion that "the state secrets privilege will not prevent plaintiffs from receiving at least some evidence tending to establish the factual predicate for the injury-in-fact underlying their claims directed at AT&T's alleged involvement in the monitoring of communication content." 439 F. Supp. 2d at 1001. With respect, the Court's conclusion in *Hepting* as to the impact of the state secrets privilege on the plaintiffs' standing was in error. By focusing solely on the issue of AT&T's alleged involvement, the Court disregarded the critical factual issue related to standing: whether the *individual plaintiffs* had in fact been subjected to the alleged intelligence activities. That issue exists apart from whether AT&T had any involvement in the

1. (U) Plaintiffs Cannot Establish Standing Because The State Secrets Privilege Forecloses Litigation Over Whether They Have Been Subject To Surveillance.

(U) The state secrets privilege precludes the named Plaintiffs from demonstrating that they personally have been subject to surveillance activities. As explained in non-classified terms by the DNI and NSA Director, the United States cannot confirm or deny whether any individual is subject to alleged surveillance activities without causing potentially grave harm to the national security, including by tending to reveal actual targets, sources, or methods. For example, if the NSA were to confirm in this case and others that specific individuals are not targets of surveillance, but later refuse to comment (as it would have to) in a case involving an actual target, a person could easily deduce by comparing such responses that the person in the latter case is a target. *See* Public McConnell Decl. ¶ 13; Public Alexander Decl. ¶ 14.

(U) The harm of revealing targets of foreign intelligence surveillance is obvious. If an individual knows or suspects he is a target of U.S. intelligence activities, he would naturally tend to alter his behavior to take new precautions against surveillance. Revealing who is not a target, in turn, would indicate who has avoided surveillance and who may be a secure channel for communication. Such information could lead a person, secure in the knowledge that he is not under surveillance, to help a hostile foreign adversary convey information; alternatively, such a person may be unwittingly utilized or even forced to convey information through a secure channel. Revealing which channels are free from surveillance and which are not would also reveal sensitive intelligence methods and thereby could help any adversary evade detection. *See* Public McConnell Decl. ¶ 13; Public Alexander Decl. ¶ 14. The consequences of identifying

---

alleged activities, because if Plaintiffs were not injured, they could not establish their standing regardless of whether AT&T, or any other telecommunications company, assisted the NSA.

who is and is not subject to alleged surveillance activities may vary depending on the circumstances. It is important to realize, however, that even a small piece of information related to one individual Plaintiff could represent, to a sophisticated adversary, an important "piece of the puzzle" of U.S. intelligence operations. *See Halkin I*, 598 F.2d at 8-9 ("The significance of one item of information may frequently depend upon knowledge of many other items of information[,]" and "what may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context.").

(U) Courts have consistently refused to recognize standing to challenge a Government surveillance program where, as here, the state secrets privilege prevents a plaintiff from establishing, and the Government from refuting, that he actually was subject to surveillance. In *Halkin I*, for example, a number of individuals and organizations claimed that they were subject to unlawful surveillance by the NSA and CIA (among other agencies) due to their opposition to the Vietnam War. *See* 598 F.2d at 3. The D.C. Circuit upheld an assertion of the state secrets privilege regarding the identities of individuals subject to NSA surveillance, rejecting the plaintiffs' argument that the privilege could not extend to the "mere fact of interception," *id.* at 8, and despite significant public disclosures about the surveillance activities at issue, *id.* at 10. As the D.C. Circuit recognized, the "identification of the individuals or organizations whose communications have or have not been acquired presents a reasonable danger that state secrets would be revealed . . . [and] can be useful information to a sophisticated intelligence analyst." *Halkin I*, 598 F.2d at 9.

(U) A similar state secrets assertion with respect to the identities of individuals subject to CIA surveillance was upheld in *Halkin II.* See 690 F.2d at 991. There, as here, the plaintiffs claimed that alleged NSA surveillance of their communications violated the Fourth Amendment. Plaintiffs claimed that their names were included on "watchlists" used to govern

NSA surveillance, arguing that this fact demonstrated a "substantial threat" that their communications would be intercepted. *See id.* at 983-84, 997. The D.C. Circuit affirmed dismissal of the Fourth Amendment claim, "hold[ing] that appellants' inability to adduce proof of actual acquisition of their communications" rendered them "incapable of making the showing necessary to establish their standing to seek relief." *Id.* at 998. As here, plaintiffs "alleged, but ultimately cannot show, a concrete injury" in light of the Government's invocation of the state secrets privilege. *Id.* at 999.[15] The court thus found dismissal warranted, even though the complaint alleged actual interception of plaintiffs' communications, because the plaintiffs' alleged injuries could be no more than speculative in the absence of their ability to prove that such interception occurred.[16] *Id.* at 999, 1001; *see also Ellsberg*, 709 F.2d 51 (also holding that dismissal was warranted where a plaintiff could not, absent recourse to state secrets, establish that he was actually subject to surveillance).

(U) In addition to foreclosing Plaintiffs' ability to prove standing for their constitutional claims, the state secrets privilege precludes Plaintiffs from establishing standing as to their statutory claims. For example, although Plaintiffs seek relief under the Foreign Intelligence

---

[15] **(U)** See *Halkin II*, 690 F.2d at 990 ("Without access to the facts about the identities of particular plaintiffs who were subjected to CIA surveillance (or to NSA interception at the instance of the CIA), direct injury in fact to any of the plaintiffs would not have been susceptible of proof."); *id.* at 987 ("Without access to documents identifying either the subjects of . . . surveillance or the types of surveillance used against particular plaintiffs, the likelihood of establishing injury in fact, causation by the defendants, violations of substantive constitutional provisions, or the quantum of damages was clearly minimal.").

[16] **(U)** Because the CIA conceded in *Halkin II* that nine plaintiffs were subjected to certain types of non-NSA surveillance, the D.C. Circuit held that *those* plaintiffs had demonstrated an injury-in-fact. *See* 690 F.2d at 1003. Nonetheless, the nine plaintiffs were precluded from seeking injunctive and declaratory relief because they could not demonstrate the likelihood of future injury or a live controversy in light of the fact that the CIA had terminated the specific intelligence methods at issue. *See id.* at 1005–09.

Surveillance Act ("FISA"), 50 U.S.C. § 1810, *Shubert* Amended Compl. ¶¶ 97-100, FISA authorizes only an "aggrieved person" to bring a civil action challenging the acquisition of communications contents. 50 U.S.C. §§ 1801(f), 1810. To ensure that this term would be "coextensive [with], but no broader than, those persons who have standing to raise claims under the Fourth Amendment with respect to electronic surveillance," H.R. Rep. No. 95-1283, at 66 (1978), Congress defined "aggrieved person" to mean one "whose communications or activities were *subject to* electronic surveillance," 50 U.S.C. § 1801(k) (emphasis added). Litigants who cannot establish their status as "aggrieved persons" therefore do "not have standing" under "any" of FISA's provisions. H.R. Rep. No. 95-1283, at 89-90; cf. *United States v. Ott*, 827 F.2d 473, 475 n.1 (9th Cir. 1987); *see also Dir., Office of Workers' Comp. Programs v. Newport News Shipbuilding & Dry Dock Co.*, 514 U.S. 122, 126 (1995) ("aggrieved" is a well-known term of art used "to designate those who have standing").

(U) Similarly although Plaintiffs seek relief under the Wiretap Act, 18 U.S.C. § 2510, *Shubert* Amended Compl. ¶¶ 101-104, that statute specifies that civil actions may be brought by a "person whose . . . communication *is* intercepted, disclosed, or intentionally used." 18 U.S.C. § 2520(a) (emphasis added). The Stored Communications Act, which Plaintiffs also invoke, *see Shubert* Amended Compl. ¶¶ 105-108 (citing 18 U.S.C. § 2707), likewise limits its civil remedies to "person[s] aggrieved" under that statute, *id.* § 2707(a); *see id.* § 2711(1) (adopting § 2510(11) definition of "aggrieved person" as one "who was a party to any intercepted . . . communication" or "a person against whom the interception was directed"). Each of these provisions reflects the fundamental point that only persons whose rights were injured by the actual interception or disclosure of their own communications (or records) have standing. Put simply, to recover damages, a plaintiff has to show that his or her rights were injured—and that cannot be done here.[17]

(U) With respect, we disagree with the Court's statement in *Hepting* that allowing further proceedings, such as discovery, before assessing the full impact of the state secrets privilege would be consistent with *Halkin* and *Ellsberg*. *See Hepting*, 439 F. Supp. 2d at 994. In *Halkin I*, the Government immediately moved to dismiss on state secrets grounds to protect facts such as those at issue here—whether the plaintiffs were subject to surveillance and the methods and techniques by which communications were intercepted. *See* 598 F.2d at 4-5. The Government also opposed discovery requests, and responded to court-propounded inquires with a state secrets privilege assertion. *See id.* at 6. The district court upheld the claim of privilege and dismissed the case as to one surveillance program (called MINARET), but denied dismissal as to a separate program (called SHAMROCK) as to which some information had been made public in Congressional hearings. *See id.* at 5. The Court of Appeals upheld the privilege assertion and dismissal as to the MINARET program and *reversed* the district court and upheld the privilege assertion as to the SHAMROCK program. *See* 598 F.2d at 8-11. Specifically with respect to discovery, the Court of Appeals said:

> In the case before us the acquisition of the plaintiffs' communications is a fact

---

[17] **(U)** It should also be noted that Plaintiffs offer no statutory basis for these claims to the extent they seek money damages against the United States. FISA, 50 U.S.C. § 1810, provides a cause of action only against "persons," *i.e.*, "individual[s]," *id.* § 1801(m), and not against the sovereign. Both the Wiretap Act and the section of the Stored Communications Act cited by Plaintiffs specifically create causes of action only against persons or entities "*other than the United States*." 18 U.S.C. § 2520(a); 18 U.S.C. § 2707(a) (emphasis added). Plaintiffs do not rely on 18 U.S.C. § 2712, which creates a cause of action for damages against the United States; nor could they do so as that section requires the exhaustion of administrative remedies prior to the commencement of suit. *Id.* § 2712(b). Accordingly, because money damages cannot be sought against the United States absent an express waiver of sovereign immunity for that purpose, *Dept. of the Army v. Blue Fox, Inc.*, 525 U.S. 255, 260 (1999), any claims for money damages against the United States, or against the named federal officials in their official capacities, must be dismissed for lack of jurisdiction.

> vital to their claim. No amount of ingenuity of counsel in putting questions on discovery can outflank the government's objection that disclosure of this fact is protected by privilege. Thus, in these special circumstances, we conclude that affording additional discovery for the government to parry plaintiffs' requests would be fruitless. *In camera* resolution of the state secrets question was inevitable.

Halkin I, 598 F.2d at 6-7. As a result of this ruling, the claims against the NSA challenging the alleged surveillance of the plaintiffs were dismissed on remand without any discovery. *See Halkin II*, 690 F.2d at 984.

(U) A separate claim proceeded against the CIA for allegedly providing "watchlisting" information to the NSA that was used to undertake surveillance. *See Halkin II*, 690 F.2d at 984. While some document discovery occurred as to the defunct surveillance program at issue, which had been the subject of a Congressional investigation, the CIA nonetheless successfully asserted the state secrets privilege as to several facts, including whether any of the plaintiffs' names had been submitted on any watchlists to the NSA. *See id.* at 985. The district court concluded that, since the very fact of any interception was protected by NSA's state secrets assertion, the plaintiffs would be unable to prove any liability on the part of CIA, and thus dismissed those claims. The Court of Appeals affirmed, again upholding the state secrets privilege to bar disclosure of the identities of individuals subject to surveillance, *see id.* at 988-89, 993 n.57, and affirming dismissal for lack of standing, *see id.* at 997-1000. *See also id.* at 998 ("Since it is the constitutionality of such interceptions that is the ultimate issue, the impossibility of proving that interception of any [plaintiff's] communications ever occurred renders the inquiry pointless from the outset."). Thus, *Halkin II* supports dismissal of claims challenging alleged surveillance on state secrets grounds and without discovery. Whatever discovery that did occur in *Halkin* was irrelevant and wasteful, because the threshold fact of whether the plaintiffs had been subject to surveillance could not be disclosed. Similarly, with respect to those plaintiffs in *Ellsberg* whom the government had not admitted overhearing, the court found that they lacked an essential element of their proof of standing and that dismissal of their claims was therefore proper. *See* 709 F.2d at 65.

(U) The same result is required here. As the cases cited above demonstrate, Plaintiffs cannot file a lawsuit alleging unlawful foreign intelligence surveillance and then seek, in the first instance, to discover whether they have actually been subject to such surveillance. Instead, where, as here, the compelling Government interest in the Nation's security requires the protection of information that tends to confirm or deny whether any individual has been the target of surveillance, litigation over the Plaintiffs' standing is foreclosed and their claims cannot proceed for lack of jurisdiction.

2. (U) Plaintiffs Cannot Establish Standing On The Basis Of A "Dragnet" Theory of Surveillance.

(U) It bears specifically noting that Plaintiffs' allegation of a "dragnet" of surveillance by the NSA—the interception of millions of domestic and international communications made by ordinary Americans, *see, e.g. Shubert* Amended Compl. ¶¶ 4, 56, 61, 80—does not establish their standing. Even if that allegation were sufficient to avoid dismissal on the pleadings, facts concerning whether Plaintiffs have been subject to any such "dragnet" of surveillance would obviously be essential to adjudicate their standing.

(U) As an initial matter, the Plaintiffs have *not* alleged that their communications have been intercepted under the Terrorist Surveillance Program acknowledged by the President. Indeed, the Plaintiffs' Amended Complaint avoids any suggestion that Plaintiffs might fall within the acknowledged and limited scope of the TSP.[18] Moreover, the Court has already recognized that, in acknowledging that the TSP was a limited program, the Government denied that it was conducting the type of domestic content "dragnet" that Plaintiffs allege. *See Hepting*, 439 F. Supp. 2d at 996. In order to prove their standing in response to the Government's motion, therefore, the named Plaintiffs are required to come forward with specific evidence rebutting the Government's denial and establishing that they personally were subject to content surveillance. But that cannot be done in light of the state secrets assertion. As previously explained, the DNI has asserted the state secrets privilege over any information tending to confirm or deny whether Plaintiffs were subject to surveillance, as well as operational information about the TSP that Plaintiffs likely would want disclosed to test, as an evidentiary matter, the limited scope of that program. Because none of that information can be disclosed without revealing intelligence targets, sources, and methods, Plaintiffs are not able to prove that they personally were subject to surveillance (either under the TSP or their alleged domestic "dragnet"). Similarly, in light of the privilege, Defendants are not able to offer evidence that would demonstrate any lack of standing. Accordingly, the Government's motion to dismiss or, in the alternative, for summary judgment must be granted.

---

[18] **(U)** Accordingly, even if Plaintiffs did purport to challenge the TSP, they would lack standing to do so on the face of their complaint.

[REDACTED TEXT]

B. (U) The Disclosure of Facts Concerning the Alleged NSA Intelligence Activities Is Required to Adjudicate Plaintiffs' Claims on the Merits.

(U) As with the threshold issue of standing, Plaintiffs cannot prove the merits of their case without establishing the existence of the alleged activities and that they are personally subject to such activities—all of which is precluded by the state secrets privilege. Even assuming *arguendo* that these threshold facts could be established (a possibility the Government disputes), the merits of Plaintiffs' claims also could not be adjudicated without facts about the operation of any alleged activity, including the precise nature of the activities, how they were conducted, why they were conducted, when they were conducted and for how long, and the intelligence value of the activities.

1. (U) Plaintiffs' Allegation that the NSA Operates a Content Collection "Dragnet" Cannot be Adjudicated Without State Secrets.

(U) This lawsuit commenced after media reports in December 2005 alleged that the NSA was engaged in certain surveillance activities. *See Shubert* Amended Compl. ¶ 50; *see also Hepting*, 439 F. Supp. 2d at 986. Plaintiffs catalogue a variety of speculative allegations concerning the purported operation of the content "dragnet" they allege to exist, many of which are drawn from equally speculative media reporting about the operation of the TSP, *see Shubert* Amended Compl. ¶¶ 4, 67-87, and cite statements made in December 2005 by the President. *Id.* ¶ 50. At that time, and in contrast to Plaintiffs' allegation of a content "dragnet" affecting "hundreds of millions of telephone, internet and email communications," *id.* ¶ 4, 80, of "millions of Americans," *id.* ¶ 2, the President stated that the TSP was limited to surveillance of communications and individuals associated with al Qaeda and did not involve the interception of purely domestic calls in the United States. *See Hepting*, 439 F. Supp. 2d at 987 (taking judicial notice of President's statement that the Government's "international activities strictly target al Qaeda and their known affiliates" and that "the government does not listen to domestic phone calls without approval" and that the Government is "not mining or trolling through the personal lives of millions of Americans") (citing 5/11/06 Statement). Then-Deputy DNI, Gen. Michael Hayden, also stated regarding the scope of the TSP:

> The purpose of all this is not to collect reams of intelligence, but to detect and prevent attacks. The intelligence community has neither the time, the resources, nor the legal authority to read communications that aren't likely to protect us, and the NSA has no interest in doing so. These are communications that we have reason to believe are al Qaeda communications, a judgment made by intelligence professionals. . . . This is targeted and focused. This is not about intercepting conversations between people in the United States. This is hot pursuit of communications entering or leaving America involving someone we believe is associated with al Qaeda.

See Remarks of Gen. Michael V. Hayden, National Press Club, Jan. 23, 2006.

(U) The crux of Plaintiffs' Amended Complaint is to ascertain whether Plaintiffs' alleged "dragnet" actually exists and covers their own communications. *See, e.g., Shubert* Amended Compl. ¶¶ 1-8, 87. As explained herein, these allegations cannot be tested without exposing state secrets; indeed, exposing alleged covert NSA intelligence activities is the very purpose of Plaintiffs' lawsuit..

(U) As a preliminary matter, we respectfully submit that the Court's conclusion in *Hepting* that the Government's acknowledgment of the existence of the TSP has "opened the door for judicial inquiry" into the matters alleged, *Hepting*, 433 F. Supp. 2d at 996, is unfounded (and is among the issues now on appeal). To the contrary, as the Court of Appeals noted in *Kasza*, the Government's public denial does not allow Plaintiffs to litigate the "veracity of the [G]overment's denial." 133 F.3d at 1172. A case involving state secrets "is not a normal case" because litigants are "denied the tools normally available for testing credibility." *Id.* Instead, the "understandably frustrating" inability of Plaintiffs to "challeng[e] the credibility of the [G]overnment's representations," is fully contemplated by the state secrets doctrine, as the Court can "satisfy itself of the credibility of the [Executive's] public declarations in the course of its *in camera* review" of classified declarations supporting the privilege. *Id.* While such materials will rarely (if ever) present the Government's full defense of a case, a court's "narrow" review of those materials can both give "utmost deference" to the Executive's representations, *id.* at 1166, while providing a circumscribed means for ensuring that the Government's denials are facially credible.

(U) Even if the Government's public denial did open the door to further inquiry, state secrets would be needed to walk through it. The President stated that TSP was a limited program that involved the surveillance of communications (1) made by parties reasonably believed to be members or agents of al Qaeda or affiliated terrorist organizations, and (2) sent to or from the United States. But proving or disproving as an evidentiary matter that the TSP was so limited and actually adjudicating Plaintiffs' "dragnet" allegation, would require the disclosure of TSP operational information and perhaps other NSA surveillance methods and activities, to show that the alleged "dragnet" of the content of millions of domestic communications is not occurring.[19] As set forth in the privilege assertions of DNI McConnell and NSA Director Alexander, those facts cannot be disclosed without causing exceptionally grave harm to national security.

[REDACTED TEXT]

(U) The foregoing demonstrates that the TSP authorized by the President after 9/11 was not directed at generalized domestic surveillance of the content of communications of millions of Americans, as Plaintiffs allege. To demonstrate that no *other* NSA program involves the alleged domestic content "dragnet," proof beyond the operation of the TSP would have to be offered to demonstrate these facts. But such information also could not be disclosed without revealing sensitive NSA sources and methods to our adversaries and thereby causing harm to the national security. Courts cannot allow litigants "to force 'groundless fishing expeditions' upon them," *Sterling*, 416 F.3d at 344, and a plaintiff is not permitted to "embark on a fishing expedition in government waters on the basis of [its own] speculation," *Ellsberg v. Mitchell*, 807 F.2d 204, 207-08 (D.C. Cir. 1986) (Scalia, Circuit Justice) ("*Ellsberg II*"). Litigation cannot proceed on claims where discovery of the actual facts needed to prove or rebut allegations is barred by the state secrets privilege. *See Molerio v. Fed. Bureau of Investigation*, 749 F. 2d 815, 826 (D.C. Cir. 1984) (it would be "a mockery of justice" to permit further proceedings where the actual facts are privileged).[20]

---

[19] **(U)** To the extent the Court in *Hepting* suggested that the proof needed to address whether or not the alleged domestic content surveillance "dragnet" exists might be found in the scope of any certification to a telecommunications carrier, *see id.* at 996-97, we again respectfully disagree. That very relationship issue is among the matters subject to the Government's privilege assertion, and to put that matter at risk in order to demonstrate that an allegation *already denied by the Government* is false, would be unfounded.

2. (U) Plaintiffs' Allegation that Certain Telecommunications Carriers Cooperated in NSA Intelligence Collection Activities Cannot be Adjudicated without State Secrets.

(U) Plaintiffs each allege that he or she was and is a customer of various telecommunications companies, *see Shubert* Amended Compl. ¶¶ 5-8, and that the NSA works with these telecommunications companies "to intercept, search and seize, and subject to electronic surveillance communications that pass through switches controlled by these companies," *id.* ¶ 70, including "email, telephone and internet [communications]." *See id.* ¶ 72. To the extent such allegations are necessary to the adjudication of Plaintiffs' claims, these allegations concerning the participation of telecommunications carrier in NSA surveillance activities can be neither proven nor denied without the use of state secrets.

(U) As the DNI and the Director of the NSA attest, the harms to national security at stake in confirming or denying an alleged intelligence relationship between the NSA and any telecommunications carrier are significant. Revealing whether or not any telecommunication carrier assists the NSA with specific intelligence activities, for example, would replace speculation with certainty for hostile foreign adversaries who are balancing the risk that a particular channel of communication may not be secure against the need to communicate efficiently. Public McConnell Decl. ¶ 16. The DNI has set forth a more than reasonable basis to conclude that harm to national security would result from the disclosure of whether the NSA has worked with any telecommunications carrier in conjunction with the alleged activities, and this Court previously has correctly observed that it is not in a position to second-guess the DNI's judgment regarding a terrorist's risk preferences—a judgment that might depend on an array of facts not before the Court. *Hepting*, 439 F. Supp. 2d at 990 , 997.

---

[20] (U) Because Plaintiffs neither allege that the TSP applies to them nor challenge that program, the lawfulness of the TSP is not at issue here. Even if they did challenge the TSP, however, classified details about the program, as well as about the threat that it was designed to address, as described in the *In Camera* Alexander and McConnell Declarations, would be needed to adjudicate its lawfulness.

[REDACTED TEXT]

(U) Thus, for the reasons comprehensively explained by the DNI and Director of the NSA, no disclosure of any information tending to confirm or deny the alleged relationship between the NSA and any telecommunications carrier can be made without compromising state secrets.

IV. (U) STATUTORY PRIVILEGE CLAIMS HAVE ALSO BEEN PROPERLY RAISED IN THIS CASE.

(U) Two statutory protections also apply to the intelligence-related information, sources and methods at issue in this case, and both have been properly invoked here. First, Section 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36, § 6, 73 Stat. 63, 64, codified at 50 U.S.C. § 402 note, provides:

> [N]othing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, of any information with respect to the activities thereof, or of the names, titles, salaries, or number of persons employed by such agency.

Id. Section 6 reflects a "congressional judgment that in order to preserve national security, information elucidating the subjects specified ought to be safe from forced exposure." *The Founding Church of Scientology of Wash., D.C., Inc. v. NSA*, 610 F.2d 824, 828 (D.C. Cir. 1979); *accord Hayden v. NSA,* 608 F.2d 1381, 1389 (D.C. Cir. 1979). In enacting Section 6, Congress was "fully aware of the 'unique and sensitive' activities of the [NSA] which require 'extreme security measures.'" *Hayden*, 608 F.2d at 1390 (citing legislative history). Thus, "[t]he protection afforded by Section 6 is, by its very terms, absolute. If [information] is covered by Section 6, NSA is entitled to withhold it . . . ." *Linder v. NSA,* 94 F.3d 693, 698 (D.C. Cir. 1996).

(U) The second applicable statute is Section 102A(i)(1) of the Intelligence Reform and

Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004), codified at 50 U.S.C. § 403-1(i)(1). This statute requires the Director of National Intelligence to protect intelligence sources and methods from unauthorized disclosure. The authority to protect intelligence sources and methods from disclosure is rooted in the "practical necessities of modern intelligence gathering," *Fitzgibbon v. CIA,* 911 F.2d 755, 761 (D.C. Cir. 1990), and has been described by the Supreme Court as both "sweeping," *CIA v. Sims,* 471 U.S. 159, 169 (1985), and "wideranging." *Snepp v. United States,* 444 U.S. 507, 509 (1980). Sources and methods constitute "the heart of all intelligence operations," *Sims*, 471 U.S. at 167, and "[i]t is the responsibility of the [intelligence community], not that of the judiciary to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the . . . intelligence-gathering process." *Id.* at 180.

(U) These statutory privileges have been properly asserted as to any intelligence-related information, sources and methods implicated by Plaintiffs' claims, and the information covered by these privilege claims are at least co-extensive with the assertion of the state secrets privilege by the DNI. *See* Public McConnell Decl. ¶ 10; Public Alexander Decl. ¶¶ 2, 12. Moreover, these privileges reinforce the conclusion that the state secrets privilege requires dismissal here, and provide an additional, independent basis for that conclusion. The fact that intelligence sources and methods, as well as information concerning NSA activities, are subject to express statutory prohibitions on disclosure underscores that the need to protect such information does not reflect solely a policy judgment by the Executive Branch, but the judgment of Congress as well.

(U) Since the Court's decision in *Hepting*, Section 6 of the National Security Act has been applied in a FOIA context to information concerning the Terrorist Surveillance Program. *See People for the American Way Found. v. NSA* ("*PFAW*"), 462 F. Supp. 2d 21 (D.D.C. 2006). In *PFAW*, the court applied Section 6 to preclude disclosure under FOIA of several categories of information related to the TSP, including the number of individuals subject to surveillance under the program, the number of communications intercepted, the identity of individuals targeted and, in particular, information that would confirm or deny whether the plaintiffs in that case had been subject to TSP surveillance—the very kind of information at issue in this case. *See id.* at 29. The court agreed that the NSA had put forward a rational explanation as to why this information should be upheld under Section 6, including that it would reveal information about NSA's success or lack of success under the TSP, as well as information about the U.S. intelligence communities capabilities, priorities, and activities. *See id.* The court also agreed that confirmation by NSA that a particular person's activities are not of a foreign intelligence interest or that NSA is unsuccessful in collecting foreign intelligence information on their activities "would allow our adversaries to accumulate information and draw conclusions about NSA's technical capabilities, sources, and methods." *See id.*

(U) The court in *PFAW* also held that Section 6 of the National Security Act does not require NSA to demonstrate what harm might result from disclosure of its activities, since "Congress has already, in enacting the statute, decided that the disclosure of NSA activities is potentially harmful." *See PFAW*, 462 F. Supp. 2d at 30 (quoting *Hayden*, 608 F.2d at 1390). Finally, the court in *PFAW* rejected the contention that, because the legality of the TSP is at issue, Section 6 does not apply to protect information about NSA activities. The court held:

> Whether the TSP, one of the NSA's many SIGINT programs involving the collection of electronic communications, is ultimately determined to be unlawful, its potential illegality cannot be used . . . to evade the "unequivocal[]" language of Section 6 which "prohibit[s] the disclosure of information relating [to] the NSA's functions and activities . . . ."

PFAW, 462 F. Supp. 2d at 31 (quoting *Linder*, 94 F.3d at 696).[21]

(U) The Court in *Hepting* essentially disregarded the Government's statutory privilege assertions. The Court observed that "[n]either of these provisions by their terms requires the court to dismiss this action. . . ." *Hepting*, 439 F. Supp. 2d at 998. That is true, but beside the point. A statutory privilege bars the disclosure of information; the consequences of that Congressional mandate are then determined in whatever proceeding the information is sought. Here, the information that Congress has barred from disclosure is central to adjudication of the case from the outset. As with the state secrets privilege, the Court's decision in *Hepting* to "determine step-by-step whether the privilege will prevent plaintiffs from discovering particular evidence," amounted to a non-decision on the substance of the statutory and state secrets privilege assertions. If, as is the case here, certain information is subject to the privilege, and if that information must be excluded under an executive privilege and by statutory law, and if as a result the case cannot proceed without that evidence, then there are no grounds for further proceedings.

---

[21] **(U)** The Court in *PFAW* also agreed that the TSP information at issue in that case was protected by the DNI's statutory privilege under 50 U.S.C. 403-1(i)(1). *See* 462 F. Supp. 2d at 31 n.8.

(U) CONCLUSION

(U) For the foregoing reasons, the Court should:

1. Uphold the United States' assertion of the military and state secrets privilege and exclude from this case the information identified in the Declarations of J. Michael McConnell, Director of National Intelligence, and Lt. Gen. Keith B. Alexander, Director of the National Security Agency; and

2. Dismiss this action or enter summary judgment for the United States because adjudication of Plaintiffs' claims requires the disclosure of state secrets and, thus, risks exceptionally grave harm to the national security of the United States.

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General

CARL J. NICHOLS
Deputy Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

s/ Anthony J. Coppolino
ANTHONY J. COPPOLINO
Special Litigation Counsel
tony.coppolino@usdoj.gov

s/ Rupa Bhattacharyya
Senior Trial Counsel
rupa.bhattacharyya@usdoj.gov

s/ Andrew H. Tannenbaum
ANDREW H. TANNENBAUM
Trial Attorney
andrew.tannenbaum@usdoj.gov
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, D.C. 20001
Phone: (202) 514-4782/(202) 514-4263/(202) 514-3146
Fax: (202) 616-8460/(202) 616-8202

Attorneys for United States of America and the Federal Defendants in their Official Capacities

DATED: May 25, 2007.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

IN RE NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION	**No. M:06-cv-01791-VRW**
	[PROPOSED] ORDER GRANTING DEFENDANTS' MOTION TO DISMISS OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT
This Document Relates Only To:	Judge: Hon. Vaughn R. Walker
Shubert v. Bush, **(Case No. 07-00693)**	

[PROPOSED] ORDER

Upon consideration of the motion of the United States and the official capacity Defendants to dismiss this action or, in the alternative, for summary judgment, the record of this case, and good cause appearing, it is

HEREBY ORDERED THAT Defendants' motion shall be and hereby is GRANTED; and it is

FURTHER ORDERED THAT this action shall be and hereby is DISMISSED.

SO ORDERED:

DATE: _______________

____
The Honorable Vaughn R. Walker
Chief Judge, United States District Court
Northern District of California